Avons-nous le choix d'utiliser l'IA en temps de guerre

Ruffo de Bonneval de la Fare des Comtes de Sinopoli de Calabre, Marie-Des-Neiges

Published in:
Cahier de la Sécurité et de la Justice

Publication date:
2020

Document Version
le PDF de l'éditeur

Avons-nous le choix d'utiliser l'IA en temps de guerre ?

Marie-des-Neiges RUFFO de CALABRE

Les possibilités d'emploi de l'IA dans le domaine militaire sont vastes, devons-nous l'utiliser à tout prix, sans analyse éthique préalable ? Si des enjeux stratégiques et légaux sont en jeu, il demeure nécessaire de respecter les deux piliers de l'éthique militaire ; la discrimination et la proportionnalité, ainsi que la tradition de la guerre juste. En outre, l'utilisation de l'IA pourrait accroître de nombreuses difficultés préexistantes : la course à l'armement, la prolifération, la dissuasion, le risque d'à nouveau user de l'arme nucléaire, de la guerre totale, des attaques préventives, et des armes de destruction massive notamment. L'IA n'est pas une technologie ***mala in se***, pour autant qu'elle ne serve pas l'autonomie du tir, à travers la construction de SALA. L'humain doit conserver non seulement un contrôle efficace sur la machine, mais aussi une supervision éclairée par des connaissances techniques et des convictions éthiques démocratiques.

Marie-des-Neiges RUFFO DE CALABRE

Marie-des-Neiges Ruffo de Calabre est docteur en philosophie (Université Paris-Sorbonne, Université de Namur), chercheur post-doc à l'université catholique de Lille au sein d'ETHICS (EA 7446), chercheur associé au Centre de recherche des écoles de St Cyr Coëtquidan (CREC), chargée d'enseignement à l'Institut catholique de Paris, chargée de cours à l'université de Namur (Belgique), membre d'ESPHIN (Espace philosophique de Namur), membre du Centre de recherche en information, droit et société (CRIDS), membre de la Complaints commission d'Euro-ISME (European Chapter of the International Society for Military Ethics), Prix de thèse IHEDN (Institut des hautes études de défense nationale), auteur d'*Itinéraire d'un robot tueur*, Éditions le Pommier, 2018.

On attribue souvent à Machiavel cette sentence : « *la fin justifie les moyens* ». Les Anglais quant à eux utilisent le proverbe « *All is fair in love and war* », pour exprimer qu'à la guerre comme en amour, tout serait permis. Parfois, l'éthique semble oubliée ou considérée comme un accessoire luxueux, un artifice de bon ton pour le public, mais sans réel impact dans les pratiques. Ainsi, il n'est pas rare de constater une volonté ferme de développer et d'user de tous les moyens possibles pour emporter la victoire. Si l'objectif visé, la victoire, ressemble à une bonne intention, pouvons-nous, en tant que nation démocratique, nous contenter de balayer les principes juridiques et éthiques, au seul motif qu'ils pourraient constituer des contraintes à l'action ? Ne devrions-nous pas plutôt étudier préventivement les conséquences éthiques et juridiques des moyens que nous développons ? Si les moyens technologiques sont majoritairement éthiquement « neutres » indépendamment de leur contexte d'emploi, qu'en est-il des capacités nouvelles liées à l'automatisation, à l'autonomie, à l'emploi du *Big Data*, de l'IA, dans le contexte si

particulier des engagements militaires ? L'ampleur de ces révolutions numériques nous laisse-t-elle encore le choix de les utiliser ? Serions-nous forcés d'en faire usage au mépris de l'éthique ?

De la possible existence de restrictions applicables à la guerre

Si, depuis le propulseur paléolithique jusqu'aux missiles balistiques intercontinentaux, l'histoire de l'armement a connu une sophistication croissante, et que selon Grossman, la guerre n'est rien d'autre que « *l'histoire de mécanismes de plus en plus efficaces pour conditionner les hommes à surmonter leur résistance innée à tuer leurs semblables*[1] », l'évolution juridique n'est heureusement pas en reste ; en témoignent les principes juridiques qui ont encadré progressivement les conflits, jusqu'aux derniers développements du droit international humanitaire (DIH), des conventions de Genève[2] et les interdictions de la CCW[3]. Le Moyen-Âge connaissait la « Trêve de Dieu », notre époque suspend théoriquement le déclenchement d'hostilités à une résolution de l'ONU. Certes, tout comme la trêve de Dieu ne fut pas toujours scrupuleusement respectée, ainsi en est-il parfois des décisions de l'ONU, comme ce fut le cas de la guerre en Irak en 2003. Cependant, loin de signifier leur inutilité, ces tentatives d'encadrer la violence pour favoriser la paix sont à considérer comme autant de pas dirigés vers davantage d'humanité, qui nous éloignent toujours un peu plus de la barbarie. Le chemin est certes encore long, certains ont parfois fait marche arrière, comme lors des nombreux génocides du XX[e] siècle, mais cela ne doit pas décourager les consciences.

Cet appel aux consciences trouve sa source dans l'éthique. L'éthique n'est pas une discipline qui idéalise les réalités pratiques au point d'en être déconnectée, sa vocation est plutôt de les inspirer. Ainsi en va-t-il du droit, comme l'illustre la clause de Martens du préambule des conventions de la Haye de 1899 et 1907. Cette dernière mentionne qu'en temps de guerre les belligérants doivent respecter notamment « *les exigences de la conscience publique* ». Le droit, inspiré par de fortes convictions éthiques préalables, régule ainsi concrètement la conduite dans la guerre. Les tribunaux seront ainsi « armés » pour rendre justice[4] après les hostilités. Inspiré par ces convictions, le droit viendra sanctionner ce que l'éthique ne pouvait que défendre.

Si le non-respect ponctuel des principes éthiques et juridiques ne doit pas ébranler la conviction qu'il est possible d'humaniser la guerre, c'est aussi en raison de la finalité même de celle-ci. En effet, la guerre n'a pas vocation de durer, au contraire de la paix qu'elle est censée assurer. La tradition éthique dite « de la Guerre Juste » complète aujourd'hui utilement le *Jus in Bello*, c'est-à-dire le droit durant la guerre, d'un *Jus post Bellum,* c'est-à-dire le droit après la guerre. Le discours prononcé à l'ONU le 14 février 2003 par le ministre des Affaires étrangères français, Dominique de Villepin, pour s'opposer au déclenchement de la guerre en Irak, illustre notamment ce lien : « *N'oublions pas qu'après avoir gagné la guerre, il faut construire la paix*[5] ». S'il est nécessaire de prendre garde à la conformité éthique des moyens que l'on déploie même en temps de guerre, et à la manière dont on usera de ces moyens, c'est bien en raison de l'exigence d'assurer une paix durable par la suite.

Pour gagner une guerre, il ne suffit pas d'une victoire militaire, fût-elle écrasante, mais aussi un traité de paix équitable. Les conditions du traité de Versailles conjuguées à la crise économique de 1929 entre autres ont déclenché en Allemagne une volonté de revanche qui suscitera la Seconde Guerre mondiale. Cet exemple de non-considération du *Jus Post Bellum* ayant pour conséquence un échec pour la paix 20 ans plus tard à peine est à comparer avec les résultats du plan Marshall de 1947, qui fut préféré au plan Morgenthau, car il favorisait la reprise économique. Pourtant, ce plan supposait que même les perdants, les ennemis, le camp des combattants injustes en somme, bénéficient de ces aides économiques à la reconstruction. L'exigence éthique d'assurer la paix a surpassé la justice purement rétributive de la loi du talion, « œil pour œil, dent pour dent », pour un résultat bien supérieur. Le plan Morgenthau proposait lui que l'Allemagne soit privée de ses industries et paye des réparations aux vainqueurs. Pour comprendre ce que cela aurait représenté et pour l'anecdote historique, il est bon de savoir que cela fera bientôt neuf ans seulement que l'Allemagne a officiellement terminé de payer les réparations liées au traité de Versailles[6].

Si donc comme le disait Clausewitz « *la guerre est la continuité de la politique par d'autres moyens*[7] », la politique

(1) Royal (B.), 2008, *La conviction d'humanité, l'éthique du soldat français,* Economica, p. 24.
(2) Voir notamment l'article 36 du premier protocole additionnel aux conventions de Genève sur les armes nouvelles.
(3) Convention on Conventional Weapon, qui a notamment interdit le recours aux lasers aveuglants.
(4) Autant que possible, même si parfois des décennies après.
(5) Extrait du discours prononcé le 14 février 2003.
(6) An. « Dimanche, l'Allemagne aura fini de payer les réparations de la Première Guerre mondiale », in *Libération*, 29 septembre 2010.

doit continuer pendant et après la guerre et cette dernière ne doit pas être considérée isolément. Un des réquisits éthiques est donc de chercher à sortir du conflit, alors même qu'il est en cours. Par ailleurs, la fin des hostilités est un désir partagé par les dirigeants, les civils, et même souvent les combattants eux-mêmes. L'opinion de chacun ne diffère que sur la manière dont l'on pourrait obtenir ce résultat. N'importe quelle technologie, même la plus innovante, ne changerait pas grand-chose à ce constat.

Comment les nouvelles technologies pourraient-elles menacer l'éthique ?

Étant à présent entendu que l'éthique militaire et ses exigences ne se limitent pas au temps de guerre proprement dit, ni aux seuls militaires, et qu'il est à la fois possible, nécessaire et judicieux de respecter ses contraintes pour une paix plus stable, la meilleure guerre étant celle que l'on ne doit pas mener, que dire de l'automatisation, de l'autonomie, de l'emploi de l'IA, et du *Big Data*, lorsqu'ils sont déployés en contexte militaire ? Rappelons que les principes éthiques eux-mêmes ne seront jamais modifiés par les nouvelles technologies, mais ces innovations peuvent les menacer d'une façon potentiellement différente qu'autrefois. Ce seront donc aux doctrines d'usages des nouvelles technologies à se conformer à l'éthique, non l'inverse. Autrement, cela constituerait un recul du progrès des droits humains.

SI DONC COMME LE DISAIT CLAUSEWITZ « *LA GUERRE EST LA CONTINUITÉ DE LA POLITIQUE PAR D'AUTRES MOYENS* », LA POLITIQUE DOIT CONTINUER PENDANT ET APRÈS LA GUERRE ET CETTE DERNIÈRE NE DOIT PAS ÊTRE CONSIDÉRÉE ISOLÉMENT. UN DES RÉQUISITS ÉTHIQUES EST DONC DE CHERCHER À SORTIR DU CONFLIT, ALORS MÊME QU'IL EST EN COURS.

Quelles seraient donc les grandes menaces que font peser l'automatisation, l'autonomie, le *Big Data* et l'IA sur le respect de l'éthique ? Pour les quatre, la menace serait d'autant plus grave qu'elles seraient utilisées pour déclencher des capacités létales. D'une manière générale, le premier point, commun au *Jus in Bello* et au droit, pour déterminer la correspondance d'une technologie avec les contraintes de la théorie de la guerre juste et du DIH, consistera à vérifier le respect de deux critères traditionnels : la discrimination[8] et la proportionnalité[9]. En tous les cas, si ces systèmes commettaient des erreurs de ciblages et tuaient non pas des combattants mais des civils, il serait certain que le principe de discrimination serait violé. Quant au deuxième critère, si ces systèmes tuaient des civils non pas en raison d'une erreur de ciblage, mais d'une force de frappe trop importante, et que les dommages collatéraux s'accumulaient, on pourrait se demander si le système ne contreviendrait pas à l'exigence de proportionnalité. Ce ne sont à ce stade que des hypothèses. Le respect de ces critères seuls ne sera néanmoins pas libératoire du respect d'autres enjeux éthiques.

L'automatisation et l'autonomie

L'automatisation, comme le déclenchement d'une mine par exemple, pose déjà un problème éthique, car la réaction de l'engin ne fait pas la distinction entre un civil ou un ennemi. Pour tenter de préserver le respect du principe éthique de distinction entre combattants et non-combattants (protégés par le DIH[10]), on peut ainsi délimiter clairement la zone pour prévenir les civils de ne pas s'approcher, instaurer un barrage, etc. La limite géographique peut être posée pour protéger le civil des mines. Rappelons que seules les mines anti-véhicules sont aujourd'hui autorisées, les mines anti-personnel étant prohibées par la convention d'Ottawa de 1997. L'autonomie d'un engin se distingue de l'automatique en ce qu'elle nécessite

(7) Clausewitz (C.), 1999, *De la Guerre* (1832), trad. L.Murawiec, édition Librairie Académique Perrin, p. 46.
(8) Distinguer un combattant d'un civil.
(9) Faire usage d'une force proportionnée à l'objectif à atteindre, afin de ne pas causer de torts excessifs. Cela suppose de respecter les civils, mais aussi autant que possible leurs biens, donc de ne cibler que des objectifs militaires, etc.
(10) Droit international humanitaire. Voir l'article 48 du premier protocole additionnel aux conventions de Genève relatif à la discrimination entre civils et combattants, et l'article 50 qui suit, définissant le civil comme n'étant pas un combattant.

un traitement informatique des données reçues par son ou ses capteurs avant de déclencher une réponse, qui peut être variable. Ce traitement informatique, s'il ne fait pas intervenir un opérateur pour s'effectuer, peut mériter l'appellation « autonome » pour réaliser une tâche bien précise. Si les tâches dont il est chargé incluent l'usage d'une arme, le danger, pour l'éthique, inclut le risque précédent de non-discrimination, si le programme n'est pas capable de vérifier s'il a affaire à un combattant ou non.

Quel serait le risque d'un tir de riposte automatique ? « *Si une riposte automatique était installée, le temps de son efficacité tactique serait limité. La contre-mesure probablement adoptée par l'adversaire ne sera pas l'abandon de la lutte armée, mais l'adoption de dispositifs moins dangereux pour le sniper, et plus meurtriers pour la patrouille : poses de mines, jets de grenades, etc. À terme, le résultat du tir automatique serait un accroissement de la violence, sans gain positif en faveur du rétablissement de la paix.*[11] »

Les SALA et les drones

Si les armes dont est équipé le robot ont la capacité de tuer, ce type de système peut porter l'acronyme de SALA, pour « systèmes d'armes létales autonomes ». Dans leur acronyme, le système n'est pas forcément un UAV, *Unmanned aerial Vehicule,* autrement dit un drone. C'est la capacité d'autonomie pour déclencher le tir qui qualifie le SALA, pas sa capacité à voler ou non. Le débat fait rage pour déterminer si ces systèmes existent déjà, pour la bonne raison qu'en l'absence de consensus juridique sur leur définition, la question demeure ouverte. Plusieurs modèles actuellement existants pourraient être concernés par la future définition des LAWS, *Letal Autonomous Weapons Systems,* la version anglaise de l'acronyme SALA : le système sous tourelle Phalanx, le Harpy, ou encore le robot de Samsung déployé à la frontière entre les deux Corées, SGR-A1, pour ne citer qu'eux. La CCW étudie la conformité de ces systèmes aux principes du DIH, notamment avec la clause de Martens, tandis que certains *lobbys* et ONG comme Human Right Watch, Stop Killer Robot ou encore PAX appellent à un moratoire préventif sur ce type de systèmes. En effet, si d'aucuns affirment qu'à ce jour il n'existe pas de système actuellement utilisé sur un champ de bataille qui pourrait à la fois cibler et tirer sans l'intervention d'un humain, d'autres travaillent sur des solutions techniques qui pourraient le permettre. Ainsi par exemple, ALX Système, une société belge qui a notamment emporté le dernier NATO innovation challenge pour une solution d'interception de drones[12], a doté ses appareils d'un système de reconnaissance de formes qui identifie les humains en temps réel sur la vidéo du moniteur. Avec deux autres firmes belges, ils travaillent aujourd'hui avec General Atomics[13], le constructeur du drone Predator.

Pourtant, nous l'avons dit, le SALA n'est pas forcément un drone. Mais la capacité d'autonomie du tir pourrait s'ajouter aux autres dangers éthiques du drone. Car les risques spécifiques à l'emploi de capacités létales par des drones, même téléopérés, existent, le philosophe Grégoire Chamayou en a abondamment traité dans *Théorie du Drone*. Nous ne prétendons pas être exhaustifs, mais citons notamment la non-proportionnalité des missiles utilisés compte tenu de la cible à atteindre, la juste comparaison devant être faite entre l'usage d'un drone ou une action au sol, plutôt qu'avec le recours à un bombardier B-17. Citons aussi l'inégalité des chances entre les combattants, qui remet en question l'affirmation de Puffendorf selon laquelle le droit de tuer à la guerre n'existe que sur le fondement de la réciprocité de ce droit. Un autre risque est de tirer en dehors d'un engagement préalable, l'usage de la force militaire ressemblant alors plus pour certains à une exécution sans procès. En effet, et cette difficulté sera partagée par les SALA, il faudra rassembler des indices en amont pour déterminer qui peut être une cible légitime ou non, sans que la future victime puisse se défendre de l'accusation d'être un terroriste. Des problèmes légaux supplémentaires peuvent être liés à la manière dont sont utilisés les drones et non pas à leur technologie, songeons notamment à des tirs de drones réalisés sur le territoire de pays avec lesquels les USA ne sont pas en guerre, comme le Pakistan ou le Yémen. Ce problème juridique n'est pas spécifique à la technologie utilisée par les drones mais s'y additionne. Ceci tend à montrer qu'une fois la possibilité technique à disposition, les contraintes juridiques sont parfois « oubliées » par le détenteur de leur pouvoir. Tel l'anneau qui rend invisible, son porteur[14] pousse ce dernier à croire son impunité certaine. Pour éviter cet écueil, il peut être bon de réfléchir en amont aux risques éthiques avant de donner un outil « trop tentant » à disposition.

L'autonomie et l'IA

L'autonomie, qui consiste pour le système à réagir à son environnement en se basant sur son traitement informatique sans intervention de l'utilisateur, peut

(11) *In* Ruffo, 2019, *Robotisation militaire : enjeux militaires, éthiques, légaux,* Economica (à paraître).
(12) https://www.lecho.be/dossier/pme-wallonie/le-liegeois-alx-systems-seduit-l-otan-avec-ses-drones-autonomes/10095330.html
(13) https://www.lecho.be/actualite/archive/le-liegeois-alx-systems-retenu-par-general-atomics/10137972.html
(14) Voir le mythe de Gygès dans La République de Platon.

être soit déterminée à l'avance par une programmation définie, un algorithme – qui laissera néanmoins une part d'incertitude proportionnelle à sa complexité – soit ne préciser que l'objectif à atteindre, laissant le soin à la machine de fixer elle-même les moyens d'y arriver. Cette seconde option fait appel à l'apprentissage machine. Ce type de programmation a connu des progrès spectaculaires ces dernières années, au point que certaines techniques d'apprentissage machine (supervisées ou non, par renforcement ou par *deep learning,* etc.) sont parfois confondues dans le vocable courant sous le terme générique d'IA[15], d'autant plus que l'apprentissage peut combiner plusieurs de ces approches, plusieurs types d'algorithmes. Enfin, même si certains algorithmes peuvent servir de base à des applications différentes, chaque IA est destinée à une tâche précise. L'IA n'est pas toute-puissante ou omnisciente, certains confondant les pouvoirs de l'informatique avec de la magie ou l'action d'une divinité. Il n'existe donc pas une mais des IA, construites avec plus ou moins de biais cognitifs, et selon des buts socio-politiques variables. Une IA construite pour la Chine aurait ainsi tendance à moins protéger la vie privée que ne devrait le faire une IA destinée au marché européen. La conformité éthique du système dépendra de la manière dont elle aura été programmée, et de ce qu'on lui demande de faire. Au regard de l'éthique militaire, une IA en tant que telle n'est donc pas une technologie *mala in se*. Par exemple, la reconnaissance de formes, telles que les humains, pour secourir plus rapidement des survivants dans une zone sinistrée, peut être une bonne chose. Mais la situation est tout autre si l'on envisage un usage à finalité létale.

L'apprentissage machine nécessite à la fois une forte capacité de calcul, et beaucoup de données sur le problème à résoudre. Toutes les IA n'ont pas besoin d'être « nourries » par des données « externes », qu'elles soient réelles ou simulées, certaines peuvent « produire » les données dont elles auront besoin pour apprendre, par exemple par *Self Learning.* Ainsi pour le jeu de Go, la différence entre l'IA AlphaGo et la version AlphaGo zero, est que la seconde a seulement reçu les règles du jeu, et a appris en jouant contre elle-même, tandis que la première avait reçu des données de parties jouées entre des humains. Si, comme c'est probable dans le domaine militaire, les données nécessaires à l'apprentissage machine n'étaient pas disponibles et qu'il devenait nécessaire de se rabattre sur l'option des données simulées, la fiabilité du résultat ne serait pas garantie. Si, à l'inverse, les données sont collectées sur le terrain, il faudra en réalité beaucoup de travail d'analyse de la part des humains pour « nettoyer » ces données avant que la machine ne devienne capable de les traiter seule, une fois qu'elle aura été entraînée avec ces données « propres ». C'est en effet une évidence que la qualité d'un système informatique soit tributaire des données sur base à partir desquelles il fonctionne.

Enfin, l'emploi de l'apprentissage machine peut potentiellement laisser dans la « black box », autrement dit dans l'opacité, la manière dont la machine a procédé à sa décision. Une telle contrainte technique est en soi une porte ouverte à toutes les déviances éthiques. Certains pourraient être tentés d'arguer que ce qui ne peut être expliqué ne doit pas être justifié, et passer ainsi sous silence des actions illégales. Cependant, certaines solutions techniques existent pour tenter d'augmenter la confiance que l'on peut accorder aux décisions de la machine. Ainsi, pour la reconnaissance d'image, certaines IA peuvent indiquer les zones de l'image qui ont été prises en compte pour déterminer son étiquetage. Loin d'évacuer l'humain, ce dernier est réintégré pour valider la décision de la machine. Ceci peut s'avérer utile pour des raisons de sécurité, et plus encore pour lutter contre le piratage. En effet, dans une *adversarial attack*[16] par exemple, une image peut contenir des pixels destinés à tromper le système de reconnaissance, même si à l'œil nu l'image semble normale. Si l'IA devait être utilisée pour prendre des décisions en matière militaire et plus encore pour cibler et déclencher des tirs, elle ne devrait pas être séparée d'une supervision humaine non seulement pour des raisons éthiques que nous allons approfondir, mais aussi pour des questions de sécurité, de résistance du système aux attaques informatiques qui ne manqueront pas d'arriver.

Cela peut s'avérer utile de développer des IA pour des capacités de cyberdéfense, d'empêcher des attaques, de créer des moyens de rendre des IA hostiles inutilisables. Autrement dit, l'IA ne doit pas être pensée comme une technologie destinée à l'attaque, mais aussi comme une capacité de défense contre des attaques informatiques, que ce soit à l'aide de virus, ou d'autres IA. En effet, se reposer sur l'informatique et sur l'apprentissage en évacuant la « sentinelle » humaine, ce serait ouvrir une vulnérabilité forte à l'intox de la machine, à son piratage, voire pire, à son détournement. Apprendre à déstabiliser

(15) Différentes définitions de l'IA existent et font débat. La définition historique donnée par le Darthmouth College est celle-ci: «*to proceed on the basis of the conjecture that every aspect of learning or any other feature of intelligence can in principle be so precisely described that a machine can be made to simulate it*». Dans cet article, nous nous bornerons à considérer l'IA de la manière la plus large possible comme un ensemble de techniques de programmations, sans nous référer explicitement à sa recherche de similitude avec le raisonnement humain.

(16) Attaque contradictoire.

des IA peut, en outre, être un moyen d'en développer de plus sûres, ce qui constituerait une approche moins dangereuse pour l'éthique.

Le Big Data et l'IA

Les données « externes » pour entraîner la machine sont aujourd'hui accessibles le plus souvent grâce au *Big Data*. Le croisement des différentes bases de données existantes donne naissance à cet ensemble massif de mégadonnées qu'il devient impossible de traiter et d'exploiter par les seules capacités humaines. La seule possibilité de stocker ces données, notamment en utilisant le *Cloud*, pose des questions techniques, voire écologiques puisque les fermes de serveurs doivent être réfrigérées, etc., partant de l'idée que le tout est plus que la somme des parties, l'espoir du *Big Data*, complémentaire de l'IA, est que de nouvelles connaissances puissent apparaître. La vision globale de l'ensemble des données connues et produites permettrait peut-être de mettre à jour des corrélations inédites, ou encore la connaissance d'une masse de données gigantesque permettrait de prendre de meilleures décisions parce que fondées sur plus d'informations, etc. Si aujourd'hui Amazon ou Microsoft, des compagnies privées qui ne vendent aucun armement, intéressent les militaires, c'est notamment pour stocker des données sur des serveurs accessibles via le *Cloud*, qui seront exploitées, traitées et utilisées pour entraîner des IA.

Ainsi, l'une des premières modifications les plus radicales provoquées par l'usage de l'IA en contexte militaire paraîtra inattendue à qui ne connaît pas le droit de la guerre : dès lors que ces entreprises privées vendent des solutions technologiques aux militaires, pour en équiper des armes ou comme simple support de leur fonctionnement, elles pourraient se voir attribuer le qualificatif de cible militaire légitime, au même titre que les usines d'armements traditionnels. Si des employés peuvent avoir conscience qu'ils deviennent des cibles militaires lorsqu'ils assemblent une bombe, en est-il de même des employés qui codent derrière un ordinateur ou veillent au bon fonctionnement d'un serveur ? L'une des exigences éthiques minimale serait donc de s'assurer du plein consentement de ces employés.

Précisons que la démission de plusieurs employés de Google pour refuser que leur entreprise développe ces technologies, en particulier le projet « Maven », n'était certes pas motivée par ce risque de devenir une cible légitime, mais avant tout parce qu'ils ne désiraient pas participer à la construction d'une technologie destinée à causer des dommages à des êtres humains. Les informaticiens sont aujourd'hui de plus en plus conscients que l'usage de l'IA dans le domaine militaire, en écartant le soldat du champ de bataille au profit d'engins technologiques, a fait reculer d'autant en amont le moment de la décision humaine éthique. Pour beaucoup, la seule conscience, outre l'autorité étatique, pouvant faire barrage avant le lancement d'un système autonome létal risque d'être son concepteur.

> CELA PEUT S'AVÉRER UTILE DE DÉVELOPPER DES IA POUR DES CAPACITÉS DE CYBERDÉFENSE, D'EMPÊCHER DES ATTAQUES, DE CRÉER DES MOYENS DE RENDRE DES IA HOSTILES INUTILISABLES. AUTREMENT DIT, L'IA NE DOIT PAS ÊTRE PENSÉE COMME UNE TECHNOLOGIE DESTINÉE À L'ATTAQUE, MAIS AUSSI COMME UNE CAPACITÉ DE DÉFENSE CONTRE DES ATTAQUES INFORMATIQUES, QUE CE SOIT À L'AIDE DE VIRUS, OU D'AUTRES IA. EN EFFET, SE REPOSER SUR L'INFORMATIQUE ET SUR L'APPRENTISSAGE EN ÉVACUANT LA « SENTINELLE » HUMAINE, CE SERAIT OUVRIR UNE VULNÉRABILITÉ FORTE À L'INTOX DE LA MACHINE, À SON PIRATAGE, VOIRE PIRE, À SON DÉTOURNEMENT.

Si en revanche les entreprises privées et leurs employés acceptent consciemment de travailler pour la Défense sur des systèmes d'armes sur lesquels les militaires n'auront pas une « supervision humaine efficace », nous nous retrouvons peut-être dans une situation similaire au déploiement de milices privées. Autrement dit, l'État se déposséderait de sa puissance de coercition au profit d'acteurs non étatiques. Est-il acceptable éthiquement de déléguer le pouvoir de tuer à des individus qui ne sont pas des soldats, mais des mercenaires, avec les conséquences que cela représente au niveau du DIH[17] ? Nous pourrions nous demander dans quelle mesure les programmeurs

(17) Selon les conventions de Genève, les mercenaires ne bénéficient pas des protections juridiques des prisonniers de guerre par exemple. Voir la convention de Genève relative au traitement des prisonniers de guerre (Convention III du 12 août 1949), Protocole additionnel I, Titre III, [P. I, 46, 47].

d'entreprises civiles ne rencontrent pas certains aspects de la définition du mercenaire[18] à savoir une participation pour des motifs financiers, pour prendre part à un combat, et ne pas avoir de lien statutaire avec les parties en conflit (à déterminer selon les individus). La question est ouverte, mais permet de percevoir qu'en déléguant à la seule machine, produite par des entreprises privées, le pouvoir à la fois de sélectionner ses cibles et de tirer seule, l'État se dessaisit de son monopole de coercition légitime au profit donc des GAFA. Devrions-nous en conclure que ces derniers, battant bientôt cryptomonnaie[19], créant des solutions informatiques pour décider qui doit mourir ou non, s'arrogeant ainsi progressivement des prérogatives régaliennes, sont en passe de devenir les égaux des acteurs étatiques ? Avec quel impact pour les démocraties et les individus qui pensaient y vivre selon leurs lois ?

L'autre danger éthique de l'usage du *Big Data* et de l'IA à des fins militaires est de ne pas respecter l'un des deux principes éthiques de base, la discrimination. Si les bases de données issues de la société civile sont exploitées pour une visée militaire, on peut se demander si les civils et leurs biens, donc par extension leurs données privées, qui doivent être protégées en temps de guerre le sont encore dans la cyberguerre. En résumé, est-ce que l'utilisation des données civiles dans une IA militaire respecte le principe de discrimination ? Enfin, un autre enjeu éthique relatif au *Big Data* est le respect de la vie privée des individus, mais ceci n'est pas spécifique aux actions militaires et se poserait dans les mêmes termes pour le domaine civil.

Ainsi définis, les termes IA et *Big Data* recouvrent des techniques et des moyens divers qui pourraient donner la méta-capacité d'autonomie, différente de l'automatique, à des systèmes conçus pour accomplir certaines tâches prédéterminées. Si ces tâches incluent le ciblage et le déclenchement du tir sans intervention humaine, une ligne rouge éthique serait franchie, car il s'agirait alors de SALA. Conserver un humain dans la boucle de commandement, non seulement comme force de réaction rapide en cas d'erreur systèmes pendant son fonctionnement, mais aussi comme certification de la cible en amont, est une solution à privilégier pour continuer à développer et utiliser l'IA en minimisant les risques à la fois éthiques et sécuritaires.

De quelques dangers éthiques supplémentaires relatifs à l'emploi de l'IA en contexte militaire

La notion de responsabilité

Pourquoi les SALA constituent-ils une ligne rouge éthique à ne pas franchir ? Que ce soit grâce à une programmation prévue d'avance, par apprentissage machine, ou par d'autres techniques d'IA, la capacité d'autonomie, autrement dit la possibilité même que ce puisse être une « machine » plutôt qu'un homme qui puisse à la fois sélectionner une cible et déclencher un tir, engendre des difficultés, notamment l'apparente disparition d'un responsable humain puisqu'il n'y a personne derrière la gâchette. Mais cette disparition n'est qu'apparente. Dans les faits, la responsabilité se retrouve dès lors comme « diluée » dans la chaîne de commandement qui va de l'ingénieur informatique jusqu'à l'opérateur qui active le mode autonome en passant par le responsable politique qui a commandé ces armes et par les officiers qui en ont ordonné l'usage.

Des propositions pour fixer une limite à la responsabilité légale ont certes été proposées. Il en existe de trois sortes ; la première consiste pour le fabricant à se dégager de toute responsabilité dès que la livraison aura été effectuée. Ce dispositif n'est pas nouveau si on se fie à un document du ministère de la Défense anglais de 2011 relatif aux drones téléopérés : « *si la logique du processus actuel des* [vols] *pilotés est maintenue, les responsabilités des concepteurs auront été déchargées une fois que le système d'aéronef non habité (UAS) aura été certifié par les autorités aériennes militaires ou civiles nationales compétentes*[20] ». On peut supposer que cette possibilité serait envisagée pour des systèmes d'armes létales autonomes. La deuxième consiste à tenir pour responsable celui qui active le mode autonome de la machine. C'est la solution technique proposée par le roboticien Ronald Arkin avec le quatrième module de son « gouverneur éthique », permettant d'identifier celui qui a allumé le robot. La troisième propose que la responsabilité juridique appartienne au robot lui-même. Cette approche nécessite de créer une fiction juridique, la « personnalité électronique ». Le rapport de l'eurodéputée Mady Delvaux allait dans ce sens en 2017, même si la proposition fut

(18) Voir Tercinet (J.), 1977, « Les mercenaires et le Droit international », *Annuaire français de droit international*, volume 23, p. 269-293.
(19) Facebook lancera bientôt sa monnaie, la Libra. Précisons que certains auteurs libéraux n'assimilent pas la monnaie à une prérogative régalienne.
(20) Ministry of Defense, «The UK approach to unmanned aircraft system», *Joint doctrine Note 2/11*, 30 mars 2011, p 5-6.

critiquée notamment par Nathalie Nevejans[21]. Cependant, quelles que soient les critiques que l'on puisse adresser à chacune de ces trois approches, elles ne sont relatives qu'à l'aspect légal de la responsabilité, laissant de côté l'existence de la responsabilité morale.

Cette apparente dilution de la responsabilité morale le long de la chaîne de commandement ne doit pas être perçue comme une « évaporation » de celle-ci, mais bien plutôt comme une teinture tenace, qui se répandrait sur tout ce qui entre en contact avec elle. En cas de morts involontaires provoquées par la machine, est-ce que les solutions légales énoncées plus haut satisferaient les familles de victimes ? Peut-être leur verserait-on des indemnités, mais la demande de justice ne serait-elle qu'une question d'argent ? Sans humain pour endosser la responsabilité, quelle place y aurait-il pour que les familles entendent des remords, des excuses, souvent psychologiquement plus cruciales à entendre que la condamnation ? Quelle place pour le pardon ou l'oubli, si nécessaires dans le *Jus Post Bellum* ? Sans humain pour combattre, il n'y aura pas d'homme pour faire la paix.

Le Targetting killing

L'emploi des drones présentait un second inconvénient qui risque d'être partagé avec l'usage de l'IA, le *targetting killing*. S'il s'agit d'une guerre asymétrique, déterminer si une personne appartient à un réseau terroriste ou non semble plus complexe que d'observer la couleur des uniformes ennemis avant de tirer, comme au temps des guerres napoléoniennes. Il y a fort à parier que l'IA sera utilisée pour traiter des informations afin de se renseigner *a priori* sur la future cible. On peut être dès lors inquiet de la sélection des futurs critères qui qualifieront une cible. Le cas de l'algorithme *Skynet* de la NSA pose question à ce sujet[22]. Edward Snowden a révélé que la NSA utilisait cet algorithme d'apprentissage au Pakistan. Utilisant les données téléphoniques et le *Big Data*, il est destiné à repérer des terroristes à partir d'un *pattern* de comportements. S'il est difficile de ne pas se voir accorder un crédit par un algorithme parce qu'une variable de notre dossier fait chuter notre « cotation », que dire de la fixation d'une « note » et d'un seuil critique, équivalent pour l'individu à un arrêt de mort, décrété par une machine, sur base de lois statistiques ? Encore faut-il avoir confiance dans la programmation de l'algorithme. En ce qui concerne *Skynet,* le directeur de Human Right Data Analysis Group, Patrick Ball, a pour sa part, «*described the NSA's methods as "ridiculously optimistic" and "completely bullshit"* [23]». Outre les biais cognitifs que l'on peut craindre dans n'importe quel algorithme, il existera aussi toujours des cas particuliers. Ainsi, un journaliste d'Al Jazeera a été étiqueté par erreur par le programme de la *NSA* comme étant un terroriste.

Ce cas ne sera sans doute pas unique, en effet les algorithmes sont confrontés à un écueil mathématique, soit ils seront programmés pour sélectionner un ensemble ne contenant que des terroristes potentiels, et certains passeront inévitablement hors du filet, soit ils seront programmés pour n'en manquer aucun, et dans ce cas ils engloberont inévitablement des innocents, ce que l'on appelle autrement des « faux positifs ». Face à un tel dilemme, il serait bon que l'humain demeure l'expert qui vérifiera les critères de « tri », et fera la distinction finale pour épargner les innocents, à la fois *a priori* dans l'établissement d'une *black list*, mais aussi au moment de presser la gâchette s'il s'agit de reconnaissance de forme. Cependant, même cette garantie n'est pas certaine si l'humain fait trop confiance à la machine – en raison peut-être d'un complexe d'infériorité vis-à-vis de ces capacités de calcul. L'exemple réel du journaliste d'Al Jazeera nous enseigne une chose ; laissé seul, un algorithme proposera certainement des faux positifs, mais le danger le plus inquiétant est que l'humain ayant rapporté ce cas l'ait présenté comme un succès de la machine. Nous trouvons donc deux dangers : laisser la machine décider seule, ou oublier que notre rôle n'est pas de la croire mais de vérifier ce qu'elle nous dit, au risque sinon de revenir au premier cas de figure. La supervision humaine efficace nécessite que nous fassions usage de notre capacité critique, plus que jamais.

La décision stratégique

Quel pourrait être un très mauvais usage de l'IA ? Laisser une intelligence artificielle décider du futur déclenchement des conflits. Certains auteurs ont étudié l'histoire pour tenter de déterminer la probabilité d'une guerre. Ainsi, Graham Allison, inspiré par ce qu'il appelle le « *piège de Thucydide*[24] », étudie la probabilité d'une guerre entre la Chine et les USA. Son étude portait sur seize cas historiques similaires antérieurs où la montée d'une

(21) Nevejeans (N.), 2016, *Traité de droit et d'éthique de la robotique civile*, LEH édition, Bordeaux, Coll. « Science, éthique et société », préfaces J. Hauser et J.-G. Ganascia, décembre.
(22) Cet algorithme ne semble pas non plus unique en son genre, on cite également le cas de «MonsterMind».
(23) Grothoff (C.), Porup (J.M.), 2016, «The NSA's SKYNET program may be killing thousands of innocent people», *Arstechnica,* 16 février.
(24) Graham (A.), 2019, *Vers la guerre, la chine et l'Amérique dans le piège de Thucydide ?*, Paris, éditions Odile Jacob.

nouvelle puissance faisait peur à la puissance établie au point de rendre la guerre inévitable. Mais Graham n'a pas l'intention d'utiliser ces connaissances pour programmer une IA. Le faible nombre de données, seize cas, serait insuffisant pour entraîner l'apprentissage d'une IA. Ceux qui possèdent un minimum de connaissances statistiques savent qu'il s'agit d'un échantillon trop petit pour être représentatif. Le risque serait de décider de se fonder malgré tout sur ces seuls cas pour programmer un algorithme, voire les compléter par des données simulées, dont la fiabilité peut être interrogée. L'opacité en outre des procédés soit pour des raisons de fonctionnement mathématiques, soit pour des raisons de secret-défense, qui auront mené à ces résultats, pose de graves questions éthiques et démocratiques. Treize des seize cas ayant résulté en une guerre entre les deux puissances, un algorithme programmé sur ces données déciderait inévitablement de déclencher une guerre lui aussi. Ceci contreviendrait à deux autres principes issus du *Jus ad Bellum*, à savoir ne déclencher une guerre qu'en dernier recours et seulement par une autorité compétente. Imaginer un jour qu'un algorithme puisse décider seul de déclencher une guerre serait une absurdité éthique, politique, démocratique et diplomatique.

Et pourtant, il existe déjà des logiciels destinés à aider à la décision stratégique en situation d'incertitude. Si l'on compare certaines actions à la guerre comme des « coups de poker », l'expression risquerait bien de décrire le futur de la réflexion stratégique. En effet, il existe différentes IA capables de jouer au poker[25], donc de bluffer les humains, et les plus avancées comme *Pluribus* gagnent même dans des parties à 6 joueurs. « L'ancêtre » *de Pluribus,* l'IA *Libratus,* a été vendue à l'armée américaine pour 10 millions de dollars[26]. L'objectif déclaré étant bien d'aider à la décision stratégique. Même en conservant une supervision humaine, de tels systèmes ne devraient être manipulés qu'avec précaution si l'on veut laisser une chance à la paix et aux manœuvres diplomatiques.

Si le risque de laisser un logiciel décider seul de tirer et de cibler posait des questions éthiques, le type d'arme qui pourrait être lancé n'avait pas été spécifiquement abordé. Or, depuis la création de missiles hypersoniques dotés de capacités nucléaires, il semble que l'emploi d'une IA autonome pour décider du tir nucléaire soit sérieusement envisagé par les USA. « *Sur le terrain, elle devrait essentiellement tourner autour de l'arrimage à l'intelligence artificielle du macro-système NC3.* […] *on imagine que l'entrée en scène de l'intelligence artificielle devrait mettre de côté les intervenants du centre de contrôle commande que sont le président des États-Unis et l'Autorité de commandement national*[27] ». Selon ce scénario, on confierait donc les codes nucléaires à une IA.

Certains affirmeront que la sécurité en serait augmentée, car cela minimiserait les risques de perte des codes par la distraction tout humaine des présidents[28]. D'autres affirmeront qu'il s'agit d'une nécessité pour répondre plus vite encore aux attaques, car le temps de réponse est réduit, et d'assurer ainsi la possibilité de la « seconde frappe ». Quelques autres rappelleront un précédent historique qui aurait pu rester inconnu de tous, à savoir la décision du lieutenant-colonel Stanislav Petrov d'aller à l'encontre du système d'alerte Oko. « "*J'ai eu une drôle de sensation dans le ventre." C'est par ces mots que Stanislav Petrov explique au Washington Post, en 1999, comment il a décidé de ne rien faire ce 26 septembre 1983, alors que les écrans de contrôle d'un bunker secret près de Moscou, indiquent que cinq missiles américains foncent sur l'URSS*[29] ». Ignorant l'alarme déclenchée par Oko, Stansislav Petrov a douté de son exactitude et s'est ainsi abstenu de déclencher la Troisième Guerre mondiale. L'alarme n'était due qu'à une erreur technique : « *Le système de surveillance a mal interprété la réflexion des rayons du soleil sur les nuages, confondue avec le dégagement d'énergie des missiles au décollage*[30] ». Bien entendu, le faible nombre de missiles a fait douter Petrov, mais ce qu'il faut pointer, ce sont les raisons pour lesquelles il a pu douter. « *C'est une chance que ce soit lui, qui a étudié l'ingénierie à Kiev, à l'École supérieure de radiotechnique des forces armées soviétiques, de service ce soir-là. "Mes collègues étaient des soldats professionnels, on leur a appris à obéir et appliquer les ordres." Ils n'auraient peut-être pas soupçonné comme lui, une erreur technique.*[31] ».

Ce que nous enseignent ces différents exemples, c'est que la machine peut faire des erreurs, pour des raisons techniques ou autres. L'humain ne doit pas la croire ou lui faire confiance, mais il doit la superviser, ce qui ne sera possible que si l'humain en question est capable de douter du bon fonctionnement de la machine et des résultats qu'elle lui propose, mais ne doit jamais lui imposer. Ceci

(25) *DeepStack, Libratus* et *Pluribus* notamment.
(26) https://www.androidpit.fr/libratus-le-joueur-de-poker-recrutement-armee-americaine
(27) https://intelligence-artificielle.developpez.com/actu/275940/Des-experts-US-proposent-de-placer-l-arsenal-nucleaire-du-pays-sous-le-controle-d-une-IA-pour-pouvoir-contrecarrer-d-eventuelles-attaques-de-la-Russie-ou-de-la-Chine/
(28) http://www.lefigaro.fr/international/2010/10/22/01003-20101022ARTFIG00397-comment-bill-clinton-a-egare-les-codes-nucleaires.php
(29) https://www.ouest-france.fr/leditiondusoir/data/8962/reader/reader.html#!preferred/1/package/8962/pub/12486/page/5
(30) *Idem*.
(31) *Idem*.

n'est possible qu'en joignant à une solide formation éthique du soldat et de l'officier une compréhension fine du fonctionnement et des capacités des logiciels qui doivent le guider. La capacité de douter n'est pas naturelle, elle doit s'apprendre et s'appuyer sur une connaissance technique et éthique. La supervision humaine, pour être efficace, nécessite plus que jamais un esprit critique. L'IA ne saurait être la canne blanche d'un aveugle dans le brouillard de la guerre, ou bien si précisément, l'outil ne pourra jamais donner la vue ni la direction à suivre, et celui qui s'accrocherait à la canne blanche, pensant ainsi voir, risque de le découvrir à ses dépens.

L'IA ne devrait pas être utilisée pour écarter la réflexion de l'humain, comme si après avoir été écarté le soldat du champ de bataille on écartait désormais l'analyste du renseignement et le général de la réflexion stratégique. Outre qu'ils doivent être ceux qui devront répondre, ce qui est à l'origine du mot responsabilité, leurs capacités propres de perception, d'imagination, de résistance à l'inattendu, de créativité, de surprise seront d'autant plus des atouts dans des guerres futures qu'elles seraient menées par des machines qui apprendraient de nos mouvements prévisibles.

Dystopie : Si les IA équipaient les SALA

Ironiquement, si l'IA équipait demain des SALA, l'argumentaire de vente pourrait se résumer ainsi : « Il s'agit d'une arme écologique puisqu'elle est dotée d'un système de reconnaissance des humains, ce qui protège la nature. Elle est proportionnée, car vous pourrez vous emparer d'une ville en laissant les infrastructures intactes, seule la population est touchée. Vous ne trouverez ni résistance ni risque. Le système détermine lui-même la ville dotée de la plus haute importance stratégique et il ne vous faudra attendre que le temps nécessaire pour que les munitions de l'essaim de SALA se vident. ». Certes personne n'est assez cynique, mais le risque que l'efficacité des SALA en fasse des armes de destructions massives est réel.

Cette efficacité potentielle de l'IA incite aujourd'hui les états à opérer une course à l'IA qui n'est pas sans rappeler la course à l'armement. Quand nous nous demandons si nous avons le choix de faire usage de l'IA, c'est bien parce que certains craignent que ne pas en disposer nous placerait en position de faiblesse. C'est la stratégie de la dissuasion qui refait surface. Mais les programmes informatiques se piratent, se copient, la prolifération des IA permettant d'équiper des SALA sera beaucoup plus rapide que celle des bombes nucléaires. Sous la menace de ces acteurs imprévisibles qui se dotent d'IA, qui dit que la tentation de mener des attaques préventives ne se fera pas plus forte ? Et si une nation décide de lancer une de ces attaques, est-ce que le concept de guerre totale ne surgirait pas à son tour, parce que la machine ne connaît pas de repos et qu'elle aura la capacité de tirer jusqu'à l'extermination totale de l'espèce humaine ? Même si l'IA n'était pas reliée aux bombes nucléaires, son emploi pour déclencher des capacités létales en ferait une arme de destruction massive.

CETTE EFFICACITÉ POTENTIELLE DE L'IA INCITE AUJOURD'HUI LES ÉTATS À OPÉRER UNE COURSE À L'IA QUI N'EST PAS SANS RAPPELER LA COURSE À L'ARMEMENT. QUAND NOUS NOUS DEMANDONS SI NOUS AVONS LE CHOIX DE FAIRE USAGE DE L'IA, C'EST BIEN PARCE QUE CERTAINS CRAIGNENT QUE NE PAS EN DISPOSER NOUS PLACERAIT EN POSITION DE FAIBLESSE. C'EST LA STRATÉGIE DE LA DISSUASION QUI REFAIT SURFACE.

Conclusion

Si le drone était une technologie qui semblait donner un avantage dans les guerres asymétriques, l'IA est développée en prévision du retour d'une guerre plus traditionnelle, entre deux nations. L'IA n'est pas une technologie *mala in se,* pour autant qu'elle ne serve pas l'autonomie du tir, autrement dit qu'elle ne décide pas seule de cibler et de tirer, afin qu'elle ne serve pas la construction des SALA. Les possibilités d'emploi de l'IA dans le domaine militaire sont si vastes que nous y retrouvons dans un cocktail détonnant tous les problèmes de la course à l'armement, de la prolifération, de la dissuasion (donc le risque d'à nouveau user de l'arme nucléaire), de la guerre totale, des attaques préventives, des armes de destruction massive, mais aussi, on l'a vu, des milices privées. Nous nous retrouvons dans une situation dans laquelle l'IA en semblant concentrer le savoir grâce aux *Big Data* et à ses capacités de calcul impressionnantes semble concentrer en même temps la résurgence d'une bonne part des dangers des guerres modernes. Enfin, si l'on tire les leçons du développement des drones, on peut constater que des technologies produites par l'armée deviennent par la suite disponibles dans le monde civil. Elles peuvent

ensuite être détournées, à bas coût tout d'abord, puis avec une sophistication croissante. Le raid de drones des Yéménites sur les réserves de pétrole en Arabie saoudite en est un exemple[32]. N'oublions donc jamais que tout ce que nous développons, d'autres s'en empareront. Assurons-nous auparavant de ne développer que des systèmes en adéquation avec les règles avec lesquelles nous souhaiterions être combattus.

S'il est nécessaire d'assurer politiquement, éthiquement, que la paix viendra et durera, que dire à ceux qui ont à lutter concrètement ? Ceux-ci ne ressentent parfois pas l'utilité à long terme de se priver de moyens plus expéditifs – pour employer un euphémisme – au motif qu'ils sont in-éthiques. Si l'envie de se battre avec la même férocité que le camp d'en face fait rage dans le cœur de certains combattants, ce qui se comprend aisément, c'est précisément parce que ce manque de respect des règles semble crier vengeance, peut-être davantage encore dans des âmes pétries d'idéaux de justice que d'autres. Si ce mécanisme psychologique est connu, il masque une conséquence logique : ne pas respecter les règles éthico-juridiques existantes revient en somme à ne pas avoir de standard éthique plus élevé que ceux des terroristes, autrement dit à se conduire comme eux et à vouloir provoquer à son tour les actes qui sont précisément à l'origine de cette révolte de l'être. Le philosophe Nietzsche résumait ainsi ce risque : « *Celui qui combat des monstres doit prendre garde à ne pas devenir monstre lui-même*[33] ». Si dans la fiction certains personnages semblent assumer qu'il faille « être un monstre pour combattre des monstres », conduisant à une surenchère de violence dans les films d'action, telle n'est pas la voie de l'éthique militaire, dont le principe général pourrait être résumé par une volonté de « diminuer la violence », au sens étymologique du terme latin *violare*, ou « dépasser les limites ». Le soldat n'a ainsi pas vocation à être cruel, mais à maîtriser sa force pour respecter ces limites. Le droit français[34] fait appel à la responsabilité du militaire, tant dans son obéissance aux ordres que dans l'exercice du commandement. Tout militaire devrait désobéir à l'ordre qu'il aurait reçu de perpétrer ce qui serait un crime contre l'humanité, et aucun ne devrait jamais en donner un de la sorte. Nous l'avons rappelé, il existe dans le droit certaines restrictions à l'usage de la force, même par des militaires en temps de guerre. Elles sont issues de convictions éthiques préalables à l'établissement de cette norme. Le soldat démocratique se doit de combattre non seulement en se contentant de ne pas violer le droit, mais en adéquation avec le respect des convictions éthiques. Cette injonction exigeante n'en est pas moins réaliste, en témoigne ce militaire engagé en Somalie : « […] *il nous restera surtout la légitime fierté d'avoir combattu en homme et non en bête, avec discernement et sans haine, contre des gens qui pourtant ne nous aimaient guère* […][35] ». L'enjeu éthique du soldat se pose donc à lui-même, l'engage à la première personne, pour lui seul, dans la solitude de sa conscience. La question éthique ne se résume donc pas au respect du droit, du permis ou du défendu, mais englobe la totalité de l'individu. Quels que soient les moyens mis à sa disposition, dans l'usage qu'il en fait ou qui lui est demandé, respecte-t-il son humanité, ses convictions démocratiques, le sens de son engagement ? Tôt ou tard, il devra répondre de l'usage de la force qui lui a été confiée, car au contraire de l'IA, lui n'est heureusement pas une machine. Alors, avons-nous le choix d'utiliser l'IA en temps de guerre ? Nous devrons toujours préserver qu'il puisse y avoir un choix, pour préserver l'humanité avant, pendant, et après la guerre.

Bibliographie

Ouvrages:

ROYAL (B.), 2008, *La conviction d'humanité, l'éthique du soldat français, Paris,* Economica, 2008..

Coll., CEULEMANS (C.), DEWYN (D.), LAMBERT (D.), RUFFO (M.d.N.), WARNOTTE (P.), *Robotisation militaire : enjeux militaires, éthiques, légaux,* Paris, Economica, 2019. (à paraître).

CICR, 1907, *Convention (IV) concernant les lois et coutumes de la guerre sur terre et son Annexe : règlement concernant les lois et coutumes de la guerre sur terre*, 18 octobre 1907.

CICR, 1977, *Protocole additionnel aux Conventions de Genève du 12 août 1949 relatif à la protection des victimes des conflits armés internationaux, Protocole I*, 8 juin 1977.

(32) https://www.lesoir.be/247832/article/2019-09-16/attaque-de-drones-contre-larabie-saoudite-le-prix-du-petrole-senvole-les-etats
(33) Nietzsche (F.), 1971, *Par-delà Bien et Mal,* trad. C. Heim, aphorisme 146, Paris, Gallimard,.
(34) Article 8 du statut général des militaires.
(35) Royal (B.), *op. cit.*, p 33

CICR, 2006, *Guide de l'examen de la licéité des nouvelles armes et des nouveaux moyens et méthodes de guerre*., Mise en œuvre des dispositions de l'article 36 du protocole additionnel 1 de 1977, Comité international de la Croix Rouge, 2006.

CLAUSEWITZ (C.), 1999, *De la Guerre* (1832), trad. L.Murawiec, édition Librairie Académique Perrin., 1999

GRAHAM (A.), 2019, *Vers la guerre, la chine et l'Amérique dans le piège de Thucydide ?*, Paris, éditions Odile Jacob, 2019.

GROTHOFF (C.), PORUP (J.M.), 2016, «The NSA's SKYNET program may be killing thousands of innocent people», *Arstechnica,* 16 feévrier 2016.

MINISTRY OF DEFENSE, 2011, «The UK approach to unmanned aircraft system», *Joint doctrine Note 2/11*, 30 mars. 2011

NEVEJEANS (N.), 2016, *Traité de droit et d'éthique de la robotique civile*, LEH édition, Bordeaux, Coll. « Science, éthique et société », préfaces J. Hauser et J.-G. Ganascia, décembre 2016.

NIETZSCHE (F.), 1971, *Par-delà Bien et Mal,* trad. HEIM (C.), Paris, Gallimard, 1971.

TERCINET (J.), .1977, « Les mercenaires et le Droit international », *Annuaire français de droit international*, volume 23, 1977.

Articles :

An., 2019, « Attaque de drones contre l'Arabie Saoudite, le prix du pétrole s'envole », *Le Soir,* 16 septembre.

An., 2010, « Dimanche, l'Allemagne aura fini de payer les réparations de la Première Guerre mondiale », *Libération*, 29 septembre.

An., 2019, « Le liégeois ALX Systems retenu par General Atomics », In *L'EchoÉcho,* 19 juin.

An., 2019, « Le légeois ALX Systems séduit l'OTAN avec ses drones autonomes », *L'Écho* 11 février

MCCOURT (D.), 2019, « Libratus, l'intelligence artificielle championne de poker recrutée par le Pentagone », *Android*, 17 janvier.

RUIZ (P.), 2019, « Des experts US proposent de placer l'arsenal nucléaire du pays sous le contrôle d'une IA », *Developpez.com* , 5 septembre.

VEY (T.) 2010, « Comment Bill Clinton a égaré les codes nucléaires », *Le Figaro*, 22 octobre.

MERDIGNAC (M.), 2017, « Le Russe qui a évité une guerre nucléaire est mort », *Ouest France*, 19 septembre.